FORM PTO-1390 (REV. 5-93)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

JC04 Rec'd PCT/PTO 09 APR 2001

ATTORNEY'S DOCKET NUMBER
2345/152

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/807181

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED:
PCT/EP99/07051	22 September 1999 (22.09.99)	09 October 1998 (09.10.98)

TITLE OF INVENTION
PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

APPLICANT(S) FOR DO/EO/US
Joerg SCHWENK

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) UNSIGNED.
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and marked-up version of specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report, Preliminary Examination Report, and Form PCT/RO/101.

Express Mail No.:EL302703835US

JC08 Rec'd PCT/PTO 09 APR 2001

U.S. APPLICATION NO. (if known, see 37 CFR 1.5) 09/807181	INTERNATIONAL APPLICATION NO. PCT/EP99/07051	ATTORNEY'S DOCKET NUMBER 2345/152

				CALCULATIONS	PTO USE ONLY
17. ☒ The following fees are submitted: **Basic National Fee (37 CFR 1.492(a)(1)-(5)):** Search Report has been prepared by the EPO or JPO .... $860.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) ...... $690.00 No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) .... $710.00 Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... $1,000.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $100.00					
ENTER APPROPRIATE BASIC FEE AMOUNT =				$ 860	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$	
Claims	Number Filed	Number Extra	Rate		
Total Claims	3 - 20 =	0	X $18.00	$	
Independent Claims	1 - 3 =	0	X $80.00	$	
Multiple dependent claim(s) (if applicable)			+ $270.00	$	
TOTAL OF ABOVE CALCULATIONS =				$860	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$860	
Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$860	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$860	
				Amount to be refunded	$
				charged	$

a. ☐ A check in the amount of $__________ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288
CUSTOMER NO. 26646

(Reg. No. 36098)

SIGNATURE

Richard L. Mayer, Reg. No. 22,490
NAME

9 Apr 2001
DATE

26646
PATENT TRADEMARK OFFICE

NY0357939 v1

09/807181
JC08 Rec'd PCT/PTO 09 APR 2001
[2345/152]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	:	Joerg SCHWENK
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS
Examiner	:	To Be Assigned
Art Unit	:	To Be Assigned

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

SIR:

Kindly amend the above-identified application before examination, as set forth below.

IN THE TITLE:

Please replace the title with the following:

--PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS--.

IN THE SPECIFICATION:

Please amend the specification, including abstract, pursuant to the attached substitute specification. Also attached is a red-lined copy of the specification, indicating deleted and added sections. No new matter has been added.

IN THE CLAIMS:

Please cancel original claims 1-3, without prejudice. Please also cancel, without prejudice, claims 1 and 2 on the revised pages of the annex to the International Preliminary Examination Report.

Please add the following new claims:

4. (New) A process for establishing a common cryptographic key for n subscribers using the Diffie-Hellman process, comprising:

assigning the n subscribers respective leaves of a binary-structured tree which has a root, n leaves, is of depth $\lceil \log_2 n \rceil$ and has treenodes;

for each one of the n subscribers, generating a respective secret, the respective secret being assigned to the one of the n leaves to which the one of the n subscribers is assigned; and

establishing secrets consecutively in a direction of the root of the tree for all k nodes of the tree starting from the n leaves of the tree across an entire hierarchy of the tree, wherein two already known secrets are combined using the Diffie-Hellman process to form a new common secret, the new common secret being allocated to a common node so that a common cryptographic key for all n subscribers is allocated to a last one of tree nodes, the last one of the tree nodes being the root of the tree.

5. (New) The process as recited in claim 4, further comprising:

adding a new subscriber to the n subscribers of the tree so that there are n+1 subscribers of the tree, the adding step including:

adding two new leaves as successors to a selected one of the n leaves of the tree so that the new tree has n+1 leaves and is of depth $\lceil \log_2(n+1) \rceil$;

assigning the one of the n subscribers to whom the selected one of the n leaves is assigned one of the two new leaves and assigning the new subscriber to another one of the two new leaves, the selected one of the n leaves becoming a common node for the two new leaves; and

starting from the new leaves in a direction of the root of the tree, establishing new secrets only in those of the tree nodes which lie within a framework of the tree on a path from the two new leaves to the root of the tree.

6. (New) The process as recited in claim 4, further comprising:

excluding a selected one of the n subscribers from the tree, the excluding step including:

removing a first one of the n leaves of the tree to which the selected one of the n subscribers is assigned;

removing a second one of the n leaves, the second one of the n leaves sharing a common node with the first one of the n leaves, the common node with the first one of the n leaves becoming a new leaf assigned to the one of the n subscribers to which the second one of the n leaves is assigned; and

starting from the new leaf of the tree in a direction of the root of the tree, establishing new secrets only in those of the tree nodes which lie within a framework of the tree on a path from the new leaf to the tree root.

REMARKS

This Preliminary Amendment cancels, without prejudice, original claims 1-3 in the underlying PCT Application No. PCT/EP99/07051. This Preliminary Amendment also cancels, without prejudice, claims 1 and 2 in the revised pages of the annex to the International Preliminary Examination Report. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

The amendments to the specification and abstract reflected in the substitute specification are to conform the specification and abstract to U.S. Patent and Trademark Office rules, and do not introduce new matter into the application.

The underlying PCT Application No. PCT/EP99/07051 includes an International Search Report, issued January 27, 2000, a copy of which is included. The Search Report includes a list of documents that were considered by the Examiner in the underlying PCT application.

The underlying PCT Application No. PCT/EP99/07051 also includes an International Preliminary Examination Report, issued August 1, 2000. A translation of the International Preliminary Examination Report and annex thereto is includes herewith.

It is respectfully submitted that the present invention is new, non-obvious, and useful. Prompt consideration and allowance of the claims are respectfully requested.

Respectfully Submitted,

KENYON & KENYON

(Reg. No. 36098)

Dated: 9 April 2001

By: _____
Richard L. Mayer
Reg. No. 22,490

One Broadway
New York, NY 10004
(212) 425-7200
(212) 425-5288
CUSTOMER NO. 26646

PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

Field of the Invention

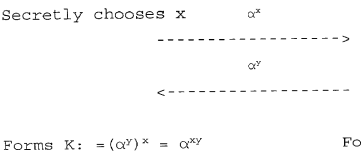
The process according to the present invention is used to generate and establish a common cryptographic key for n subscribers in order to guarantee the secrecy of messages which are to be transmitted exclusively to the n subscribers via insecure communication channels.

Background Information

The mechanisms of encryption and authentication are used to protect the confidentiality and integrity of communication between two or more persons. However, such mechanisms require the existence of shared information at all subscribers. This shared information is referred to as a cryptographic key.

A conventional process for establishing a common key via insecure communication channels is the process of Diffie and Hellman (DH process; see W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976). The basis of the Diffie-Hellmann key exchange (DH76) is the fact that it is virtually impossible to calculate logarithms modulo a large prime number p. This fact is utilized by Alice and Bob in the example shown below, in that they each secretly choose a number x and y, respectively, smaller than p (and relatively prime to p-1). They then send each other (consecutively or simultaneously) the x-th (and y-th) power of a publicly known number α. From the received powers, they are able

to calculate a common key $K:=\alpha^{xy}$ by renewed raising to the power with x and y, respectively. An attacker who sees only α^x and α^y is unable to calculate K therefrom. (The only presently known method of doing so would involve first calculating the logarithm, e.g., of α^x to the base α modulo p, and then raising α^y to that power.)



Example of Diffie-Hellmann key exchange

The problem with the DH key exchange described in the example is that Alice does not know whether she is actually communicating with Bob or with an impostor. In IPSec, this problem is solved by the use of public key certificates in which the identity of a subscriber is linked to a public key by a trustworthy authority. The identity of a conversation partner is thereby verifiable.

DH key exchange can also be implemented using other mathematical structures, e.g., using finite bodies GF(2n) or elliptic curves. Such alternatives make it possible to improve performance. However, this process is only suitable for agreeing upon a key between two subscribers.

Various attempts have been made to extend the DH process to three or more subscribers (DH groups). (An overview of the state of the art is given by M. Steiner, G. Tsudik, M. Waidner, *Diffie-Hellman Key Distribution Extended to Group Communication*, Proc. 3rd ACM Conference on Computer

and Communications Security, March 1996, New Delhi, India.)

An extension of the DH process to three subscribers A, B and C is described, for example, by the following table. (Calculation in each case mod p):

	A → B	B → C	C → A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

After carrying out these two rounds, each of the three subscribers is able to calculate the secret key g^{abc} mod p.

In all these extensions, at least one of the following three problems occurs:

- The subscribers must be arranged in a certain manner, for instance in a circle in the above example.
- The subscribers have no influence vis-à-vis the central station on the choice of key.
- The number of rounds is dependent on the number of subscribers.

A further process for the common establishment of a key is described in German Patent Application No. 195 38 385.0. In this process, however, the central station must know the secret keys of the subscribers.

In the IEEE Transaction On Software Engineering, an article dated 5/20/1998, pages 1 through 13, entitled "*Key Establishment in Large Dynamic Groups Using One-Way Function Trees*" by David A. McGrew and Alan T. Sherman, introduces a process for establishing a common cryptographic key. This process is based on a tree structure. In that case, a group manager manages a binary tree, each node x of it being linked to two cryptographic keys, a node key kx and a hidden node key $k'x=g(k_x)$. The hidden node key is calculated from the node key with the aid of a one-way function. Each subscriber knows the unhidden node keys on the path from his/her node up to the root and the hidden node keys for the nodes which are siblings for his/her path to the root, and otherwise no other hidden or unhidden keys. The feasibility of this process is based on the fact that the group manager knows all the leaf keys.

Burmester, Desmedt, *A secure and efficient conference key distribution system*, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 describes a design in which two rounds are required to generate the key, it being necessary in the second round for the central station to send n messages of length p = approx. 1000 bits for n subscribers.

Another conventional cryptographic process is referred to as the (n,t) threshold process. With an (n,t) threshold process, it is possible to break a key k down into t parts (called shadows), such that said key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie* (2nd edition), Vieweg Verlag, Wiesbaden 1998).

Summary of the Invention

The present invention can provide the establishment of a common group key between a central station and a group of n subscribers. The present invention can also provide that, even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

In accordance with the present invention, a process is provided in which a group key is established with the aid of a tree structure. To that end, the number of subscribers n involved in the key agreement is represented as a binary tree having n leaves. For each natural number n, there are one or more representations of this type. The number of leaves is identical with the number of subscribers included in the process. This means that a number of n leaves of a binary tree of depth $\lceil \log_2 n \rceil$ is allocated to a number of n subscribers.

Brief Description of the Drawings

Fig. 1 shows a tree structure for three subscribers according to an embodiment of the present invention;

Fig. 2 shows a tree structure for a key agreement for four subscribers A, B, C and D according to an embodiment of the present invention;

Fig. 3 shows a tree structure of a key agreement for five subscribers A, B, C, D and E according to an embodiment of the present invention;

Fig. 4 shows extending the tree structure by one subscriber for a further embodiment of the present invention according to Fig. 2; and

Fig. 5 shows the removal/deletion of a subscriber from the tree structure for a further embodiment of the present invention according to Fig. 2.

Detailed Description

Fig. 1 shows the operating principle of the process according to the present invention with reference to the tree structure of a key agreement for three subscribers A, B, C.

In order to establish a common key, subscribers A, B and C proceed as follows:

- Subscribers A and B carry out a DH process with randomly generated numbers a and b. They obtain the common key $k1=g^{ab}$ mod p, which is allocated to the common node K1.

- Subscribers A and B on the one side, and subscriber C on the other side carry out a second DH process which is based on common key k1 of subscribers A and B and on a randomly generated number c of subscriber C. The result is common key $k = g^{kl \cdot c}$ mod p, which is allocated to the root of tree K_w.

In the following, an example of a key agreement for four subscribers A, B, C and D is described with reference to Fig. 2:
In order to establish a common key for four subscribers (Fig. 2), subscribers A, B, C and D proceed as follows:

- Subscribers A and B carry out a DH process with randomly generated numbers a and b. They obtain the common key $k1=g^{ab}$ mod p.

- Subscribers C and D carry out a DH process with randomly selected numbers c and d. They obtain the common key $k2=g^{cd}$ mod p.

- Subscribers A and B on the one side, and subscribers C and D on the other side jointly carry out a second DH process in which subscribers A and B include key k1 and subscribers C and D include key k2. The result is common key $k_w = g^{k1k2}$ mod p, which is allocated to the root of tree K_w.

In the following, an example of a key agreement for five subscribers A, B, C, D and E is described with reference to Fig. 3:

In order to establish a common key, subscribers A, B, C, D and E proceed as follows:

- Subscribers A and B carry out a DH process with randomly selected numbers a and b. They obtain the common key $k1=g^{ab}$ mod p.

- Subscribers C and D carry out a DH process with randomly selected numbers c and d. They obtain the common key $k2=g^{cd}$ mod p.

- Subscribers A and B on the one side, and subscribers C and D on the other side jointly carry out a second DH process in which subscribers A and B include the common key k1 and subscribers C and D include the common key K2. The result is a common key $k3 = g^{k1k2}$ mod p for subscribers A, B, C and D.

- Subscribers A, B, C and D on the one side, and

subscriber E on the other side carry out a third DH process in which common key k3 of subscribers A, B, C and D and a random number e generated for subscriber E are included. The result is common key $k_w = g^{k3 \cdot e} \bmod p$, which is allocated to the root of the tree K_w.

Owing to the structure of the process according to the present invention, it is possible to include new subscribers or to exclude individual subscribers without having to carry out the entire process again for each subscriber.

The addition of a new subscriber is explained in greater detail with reference to a tree structure having four subscribers according to Fig. 4. The starting situation is a tree structure according to Fig. 2, to which a new subscriber is to be added at leaf B.

When a new subscriber is added to an already existing tree structure which possesses a common secret, in order to establish a new common key for n+1 subscribers, two new leaves B1 and B2 are added at a suitable location of the binary tree (leaf B given). The new tree then has n+1 leaves and is of depth $\lceil \log_2(n+1) \rceil$. The subscriber previously assigned to leaf B is assigned to one of the new leaves B1. The new subscriber is assigned to the other leaf B2 still free. The previous leaf B becomes a node K1 for leaves B1 and B2. Starting from new leaves B1 and B2, new secrets are established as far as the root of the tree only in those nodes K which lie within the framework of the tree structure on the path from new leaves B1 and B2 to the root of the tree K_w. In this specific case, they are nodes K1, K2 and K_w.

If the number of subscribers is a power of two, the depth

of the tree is increased through this operation by 1 (see previous example). If the number of subscribers is not a power of two, then, through skillful selection of the leaf to be divided, it is possible to avoid an increase of the depth, as shown by the following example:

In order, for example, to add a fourth subscriber to three subscribers, one proceeds as follows (starting from the situation according to Fig. 1):

- Subscriber C carries out a DH process with newly added subscriber D using randomly generated numbers c` and d (c` should differ from the previously selected c, but this need not be the case). The result is $k2` = g^{c`d} \bmod p$.

- Subscriber A and subscriber B on the one side, and subscribers C and D on the other side carry out a DH process using the values k1 and k2`. The result is $k = g^{k1 \cdot k2`} \bmod p$.

With such a configuration, subscribers A and B need not carry out a new key exchange. Generally, it is only necessary to newly agree upon the secrets which lie in the associated tree on the path from the leaf of the new subscriber to root K_w.

The exclusion or deletion of a subscriber is explained in greater detail with reference to a tree structure having four subscribers according to Fig. 5. The starting situation is a tree structure according to Fig. 2, from which subscriber B is to be removed.

When a subscriber B is excluded or deleted from an already existing tree structure which has a common

secret, then, as indicated in Fig. 5, both the leaf of subscriber B who is to be removed and the leaf of subscriber A, assigned to the same common node K1, are removed. Common node K1 becomes new leaf A' of subscriber A remaining in the tree structure. Starting from the leaves of the tree and going as far as root K_w, new secrets are established only in those nodes K which are directly affected by new leaf A' within the framework of the tree structure in the direction of root K_w. In this specific case, this is only root node K_w. Given such a configuration, subscribers C and D need not carry out a new key exchange. Generally, in this case it is also only necessary to newly agree upon those secrets which lie in the associated tree on the path from the leaf of the partner of the removed subscriber to the root.

The process can be further developed in many ways: For example, it is possible to use other groups for forming the discrete exponential function
$x \rightarrow g^x$.

When a subscriber is added or removed, it is possible, for example, to agree not to use the old secrets, but rather the result of a (possibly randomized) one-way function for the required new implementations of the DH process.

Abstract

A process is described which can be used to generate a cryptographic key for a group of subscribers whose number is subject to change. The process can further provide that even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

Field of the Invention

The process according to the present invention is used to generate and establish a common cryptographic key for n subscribers in order to guarantee the secrecy of messages which are to be transmitted exclusively to the n subscribers via insecure communication channels.

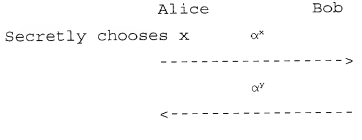
Background Information

The mechanisms of encryption and authentication are used to protect the confidentiality and integrity of communication between two or more persons. However, such mechanisms require the existence of shared information at all subscribers. This shared information is referred to as a cryptographic key.

A [known]conventional process for establishing a common key via insecure communication channels is the process of Diffie and Hellman (DH process; see W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976).

The basis of the Diffie-Hellmann key exchange (DH76) is the fact that it is virtually impossible to calculate logarithms modulo a large prime number p. This fact is utilized by Alice and Bob in the example shown below, in that they each secretly choose a number x and y, respectively, smaller than p (and relatively prime to p-1). They then send each other (consecutively or simultaneously) the x-th (and y-th) power of a publicly

known number α. From the received powers, they are able to calculate a common key $K:=\alpha^{xy}$ by renewed raising to the power with x and y, respectively. An attacker who sees only α^x and α^y is unable to calculate K therefrom. (The only presently known method of doing so would involve first calculating the logarithm, e.g. of α^x to the base α modulo p, and then raising α^y to that power.)



Example of Diffie-Hellmann key exchange

The problem with the DH key exchange described in the example is that Alice does not know whether she is actually communicating with Bob or with an impostor. In IPSec, this problem is solved by the use of public key certificates in which the identity of a subscriber is linked to a public key by a trustworthy authority. The identity of a conversation partner is thereby verifiable.

DH key exchange can also be implemented using other mathematical structures, e.g. using finite bodies GF(2n) or elliptic curves. Such alternatives make it possible to improve performance. However, this process is only suitable for agreeing upon a key between two subscribers.

Various attempts have been made to extend the DH process to three or more subscribers (DH groups). (An overview of the state of the art is given by M. Steiner, G. Tsudik, M. Waidner, *Diffie-Hellman Key Distribution Extended to Group Communication*, Proc. 3rd ACM Conference on Computer

and Communications Security, March 1996, New Delhi, India.)

[
]An extension of the DH process to three subscribers A, B and C is described, for example, by the following table. (Calculation in each case mod p):

	A → B	B → C	C → A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

After carrying out these two rounds, each of the three subscribers is able to calculate the secret key g^{abc} mod p.

In all these extensions, at least one of the following three problems occurs:

- The subscribers must be arranged in a certain manner, for instance in a circle in the above example.
- The subscribers have no influence vis-à-vis the central station on the choice of key.
- The number of rounds is dependent on the number of subscribers.

A further process for the common establishment of a key is [known from the]described in German Patent Application No. 195 38 385.0. In this process, however, the central station must know the secret keys of the subscribers.

[A design approach from]In the IEEE Transaction On Software Engineering, an article dated 5/20/1998, pages 1 through 13, entitled *"Key Establishment in Large Dynamic Groups Using One-Way Function Trees"* by David A. McGrew and Alan T. Sherman, introduces a process for establishing a common cryptographic key. This process is based on a tree structure. In that case, a group manager manages a binary tree, each node x of it being linked to two cryptographic keys, a node key kx and a hidden node key $k'x=g(k_x)$. The hidden node key is calculated from the node key with the aid of a one-way function. Each subscriber knows the unhidden node keys on the path from his/her node up to the root and the hidden node keys for the nodes which are siblings for his/her path to the root, and otherwise no other hidden or unhidden keys. The feasibility of this process is based on the fact that the group manager knows all the leaf keys.

Burmester, Desmedt, *A secure and efficient conference key distribution system*, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 [is also known,]describes a design in which two rounds are required to generate the key, it being necessary in the second round for the central station to send n messages of length p = approx. 1000 bits for n subscribers.

[Also known is a]Another conventional cryptographic process is referred to as the (n,t) threshold process. With an (n,t) threshold process, it is possible to break a key k down into t parts (called shadows), such that said key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie*_[ ](2nd edition), Vieweg Verlag, Wiesbaden 1998).

Summary of the Invention

The present [process is intended to permit]invention can provide the establishment of a common group key between a central station and a group of n subscribers. The [process is to be such]present invention can also provide that, even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

[T]In accordance with the [objective is achieved by]present invention, a process is provided in which a group key is established with the aid of a tree structure. [According to the invention, t]To that end, the number of subscribers n involved in the key agreement is represented as a binary tree having n leaves. For each natural number n, there are one or more representations of this type. The number of leaves is identical with the number of subscribers included in the process. This means that a number of n leaves of a binary tree of depth $\lceil \log_2 n \rceil$ is allocated to a number of n subscribers.

Brief Description of the Drawings

Fig. 1 shows a tree structure for three subscribers according to an embodiment of the present invention;

Fig. 2 shows a tree structure for a key agreement for four subscribers A, B, C and D according to an embodiment of the present invention;

Fig. 3 shows a tree structure of a key agreement for five subscribers A, B, C, D and E according to an embodiment of the present invention;

Fig. 4 shows extending the tree structure by one

subscriber for a further embodiment of the present invention according to Fig. 2; and

Fig. 5 shows the removal/deletion of a subscriber from the tree structure for a further embodiment of the present invention according to Fig. 2.

Detailed Description

Fig. 1 shows the operating principle of the process according to the present invention with reference to the tree structure of a key agreement for three subscribers A, B, C.

In order to establish a common key, subscribers A, B and C proceed as follows:

- Subscribers A and B carry out a DH process with randomly generated numbers a and b. They obtain the common key $k1=g^{ab}$ mod p, which is allocated to the common node K1.

- Subscribers A and B on the one side, and subscriber C on the other side carry out a second DH process which is based on common key k1 of subscribers A and B and on a randomly generated number c of subscriber C. The result is common key $k = g^{k1 \cdot c}$ mod p, which is allocated to the root of tree K_w.

[

The process according to the invention is explained in greater detail with reference to exemplary embodiments.
Fig. 2 shows the tree structure for a key agreement for four subscribers A, B, C and D.
Fig 3 shows the tree structure of a key agreement for five subscribers A, B, C, D and E.
Fig. 4, on the basis of an already existing tree

structure according to Fig. 2, shows an example for extending the tree structure by one subscriber. Fig. 5, on the basis of an already existing tree structure according to Fig. 2, shows the removal/deletion of a subscriber from the tree structure.

]

In the following, an example of a key agreement for four subscribers A, B, C and D is described with reference to Fig. 2:

In order to establish a common key for four subscribers (Fig. 2), subscribers A, B, C and D proceed as follows:

- Subscribers A and B carry out a DH process with randomly generated numbers a and b. They obtain the common key $k1=g^{ab} \bmod p$.

- Subscribers C and D carry out a DH process with randomly selected numbers c and d. They obtain the common key $k2=g^{cd} \bmod p$.

- Subscribers A and B on the one side, and subscribers C and D on the other side jointly carry out a second DH process in which subscribers A and B include key k1 and subscribers C and D include key k2. The result is common key $k_w = g^{k1 \cdot k2} \bmod p$, which is allocated to the root of tree K_w.

In the following, an example of a key agreement for five subscribers A, B, C, D and E is described with reference to Fig. 3:

In order to establish a common key, subscribers A, B, C, D and E proceed as follows:

- Subscribers A and B carry out a DH process with randomly selected numbers a and b. They obtain the common

key $k1=g^{ab} \bmod p$.

- Subscribers C and D carry out a DH process with randomly selected numbers c and d. They obtain the common key $k2=g^{cd} \bmod p$.

- Subscribers A and B on the one side, and subscribers C and D on the other side jointly carry out a second DH process in which subscribers A and B include the common key k1 and subscribers C and D include the common key K2. The result is a common key $k3 = g^{k1k2} \bmod p$ for subscribers A, B, C and D.

- Subscribers A, B, C and D on the one side, and subscriber E on the other side carry out a third DH process in which common key k3 of subscribers A, B, C and D and a random number e generated for subscriber E are included. The result is common key $k_w = g^{k3e} \bmod p$, which is allocated to the root of the tree K_w.

Owing to the structure of the process according to the present invention, it is possible to include new subscribers or to exclude individual subscribers without having to carry out the entire process again for each subscriber.

The addition of a new subscriber is explained in greater detail with reference to a tree structure having four subscribers according to Fig. 4. The starting situation is a tree structure according to Fig. 2, to which a new subscriber is to be added at leaf B.

When a new subscriber is added to an already existing tree structure which possesses a common secret, in order to establish a new common key for n+1 subscribers, two

new leaves B1 and B2 are added at a suitable location of the binary tree (leaf B given). The new tree then has n+1 leaves and is of depth $\lceil \log_2(n+1) \rceil$. The subscriber previously assigned to leaf B is assigned to one of the new leaves B1. The new subscriber is assigned to the other leaf B2 still free. The previous leaf B becomes a node K1 for leaves B1 and B2. Starting from new leaves B1 and B2, new secrets are established as far as the root of the tree only in those nodes K which lie within the framework of the tree structure on the path from new leaves B1 and B2 to the root of the tree K_w. In this specific case, they are nodes K1, K2 and K_w.

If the number of subscribers is a power of two, the depth of the tree is increased through this operation by 1 (see previous example). If the number of subscribers is not a power of two, then, through skillful selection of the leaf to be divided, it is possible to avoid an increase of the depth, as shown by the following example:

In order, for example, to add a fourth subscriber to three subscribers, one proceeds as follows (starting from the situation according to Fig. 1):

- Subscriber C carries out a DH process with newly added subscriber D using randomly generated numbers c` and d (c` should differ from the previously selected c, but this need not be the case). The result is $k2` = g^{c`d} \bmod p$.

- Subscriber A and subscriber B on the one side, and subscribers C and D on the other side carry out a DH process using the values k1 and k2`. The result is $k = g^{k1\,k2`} \bmod p$.

With such a configuration, subscribers A and B need not

carry out a new key exchange. Generally, it is only necessary to newly agree upon the secrets which lie in the associated tree on the path from the leaf of the new subscriber to root K_w.

The exclusion or deletion of a subscriber is explained in greater detail with reference to a tree structure having four subscribers according to Fig. 5. The starting situation is a tree structure according to Fig. 2, from which subscriber B is to be removed.

When a subscriber B is excluded or deleted from an already existing tree structure which has a common secret, then, as indicated in Fig. 5, both the leaf of subscriber B who is to be removed and the leaf of subscriber A, assigned to the same common node K1, are removed. Common node K1 becomes new leaf A' of subscriber A remaining in the tree structure. Starting from the leaves of the tree and going as far as root K_w, new secrets are established only in those nodes K which are directly affected by new leaf A' within the framework of the tree structure in the direction of root K_w. In this specific case, this is only root node K_w. Given such a configuration, subscribers C and D need not carry out a new key exchange. Generally, in this case it is also only necessary to newly agree upon those secrets which lie in the associated tree on the path from the leaf of the partner of the removed subscriber to the root.

The process can be [advantageously]further developed in many ways: For example, it is possible to use other groups for forming the discrete exponential function $x \rightarrow g^x$.

When a subscriber is added or removed, it is possible, for example, to agree not to use the old secrets, but rather the result of a (possibly randomized) one-way

function for the required new implementations of the DH process.

[Abstract

The process is to be such that,]

Abstract

A process is described which can be used to generate a cryptographic key for a group of subscribers whose number is subject to change. The process can further provide that even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

[According to the present invention, each of the n subscribers (I) is assigned to one leaf of a binary-structured tree which has precisely n leaves and is of depth $\lceil \log_2 n \rceil$. For each subscriber (I), a secret (i) is generated and is assigned to that leaf of the tree to which the respective subscriber (I) is also assigned. Secrets are established consecutively in the direction of the tree root for all nodes (K) of the tree, two already known secrets always being combined via the DH process to form a new common secret. The last node K_w contains the common key of all n subscribers.

The process of the present invention can be advantageously used to generate a cryptographic key for a group of subscribers whose number is subject to change.

Fig. 1]

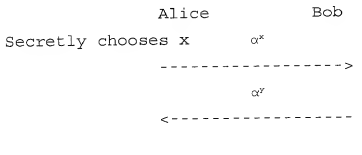
PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS

The process according to the present invention is used to generate and establish a common cryptographic key for n subscribers in order to guarantee the secrecy of messages which are to be transmitted exclusively to the n subscribers via insecure communication channels.

The mechanisms of encryption and authentication are used to protect the confidentiality and integrity of communication between two or more persons. However, such mechanisms require the existence of shared information at all subscribers. This shared information is referred to as a cryptographic key.

A known process for establishing a common key via insecure communication channels is the process of Diffie and Hellman (DH process; see W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976). The basis of the Diffie-Hellmann key exchange (DH76) is the fact that it is virtually impossible to calculate logarithms modulo a large prime number p. This fact is utilized by Alice and Bob in the example shown below, in that they each secretly choose a number x and y, respectively, smaller than p (and relatively prime to p-1). They then send each other (consecutively or simultaneously) the x-th (and y-th) power of a publicly known number α. From the received powers, they are able to calculate a common key $K:=\alpha^{xy}$ by renewed raising to the power with x and y, respectively. An attacker who sees only α^x and α^y is unable to calculate K therefrom. (The only presently known method of doing so would involve

first calculating the logarithm, e.g. of α^x to the base α modulo p, and then raising α^y to that power.)



Example of Diffie-Hellmann key exchange

The problem with the DH key exchange described in the example is that Alice does not know whether she is actually communicating with Bob or with an impostor. In IPSec, this problem is solved by the use of public key certificates in which the identity of a subscriber is linked to a public key by a trustworthy authority. The identity of a conversation partner is thereby verifiable.

DH key exchange can also be implemented using other mathematical structures, e.g. using finite bodies GF(2n) or elliptic curves. Such alternatives make it possible to improve performance. However, this process is only suitable for agreeing upon a key between two subscribers.

Various attempts have been made to extend the DH process to three or more subscribers (DH groups). (An overview of the state of the art is given by M. Steiner, G. Tsudik, M. Waidner, *Diffie-Hellman Key Distribution Extended to Group Communication*, Proc. 3rd ACM Conference on Computer and Communications Security, March 1996, New Delhi, India.)

An extension of the DH process to three subscribers A, B

and C is described, for example, by the following table. (Calculation in each case mod p):

	A → B	B → C	C → A
1st round	g^a	g^b	g^c
2nd round	g^{ca}	g^{ab}	g^{bc}

After carrying out these two rounds, each of the three subscribers is able to calculate the secret key g^{abc} mod p.

In all these extensions, at least one of the following three problems occurs:

- The subscribers must be arranged in a certain manner, for instance in a circle in the above example.
- The subscribers have no influence vis-à-vis the central station on the choice of key.
- The number of rounds is dependent on the number of subscribers.

A further process for the common establishment of a key is known from the German Patent 195 38 385.0. In this process, however, the central station must know the secret keys of the subscribers.

A design approach from Burmester, Desmedt, *A secure and efficient conference key distribution system*, Proc. EUROCRYPT'94, Springer LNCS, Berlin 1994 is also known, in which two rounds are required to generate the key, it being necessary in the second round for the central

station to send n messages of length p = approx. 1000 bits for n subscribers.

Also known is a cryptographic process referred to as the (n,t) threshold process. With an (n,t) threshold process, it is possible to break a key k down into t parts (called shadows), such that said key k can be reconstructed from any n of the t shadows (see Beutelspacher, Schwenk, Wolfenstetter: *Moderne Verfahren der Kryptographie* (2nd edition), Vieweg Verlag, Wiesbaden 1998).

The present process is intended to permit the establishment of a common group key between a central station and a group of n subscribers. The process is to be such that, even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

The objective is achieved by a process in which a group key is established with the aid of a tree structure. According to the invention, to that end, the number of subscribers n involved in the key agreement is represented as a binary tree having n leaves. For each natural number n, there are one or more representations of this type. The number of leaves is identical with the number of subscribers included in the process. This means that a number of n leaves of a binary tree of depth $\lceil \log_2 n \rceil$ is allocated to a number of n subscribers.

Fig. 1 shows the operating principle of the process according to the invention with reference to the tree structure of a key agreement for three subscribers A, B, C.

In order to establish a common key, subscribers A, B and C proceed as follows:

- Subscribers A and B carry out a DH process with

randomly generated numbers a and b. They obtain the common key $k1=g^{ab}$ mod p, which is allocated to the common node K1.

- Subscribers A and B on the one side, and subscriber C on the other side carry out a second DH process which is based on common key k1 of subscribers A and B and on a randomly generated number c of subscriber C. The result is common key $k = g^{kl \cdot c}$ mod p, which is allocated to the root of tree K_w.

The process according to the invention is explained in greater detail with reference to exemplary embodiments.
Fig. 2 shows the tree structure for a key agreement for four subscribers A, B, C and D.
Fig 3 shows the tree structure of a key agreement for five subscribers A, B, C, D and E.
Fig. 4, on the basis of an already existing tree structure according to Fig. 2, shows an example for extending the tree structure by one subscriber.
Fig. 5, on the basis of an already existing tree structure according to Fig. 2, shows the removal/deletion of a subscriber from the tree structure.

In the following, an example of a key agreement for four subscribers A, B, C and D is described with reference to Fig. 2:
In order to establish a common key for four subscribers (Fig. 2), subscribers A, B, C and D proceed as follows:

- Subscribers A and B carry out a DH process with randomly generated numbers a and b. They obtain the common key $k1=g^{ab}$ mod p.
- Subscribers C and D carry out a DH process with randomly selected numbers c and d. They obtain the common key $k2=g^{cd}$ mod p.
- Subscribers A and B on the one side, and subscribers C and D on the other side jointly carry out a second DH

process in which subscribers A and B include key k1 and subscribers C and D include key k2. The result is common key $k_w = g^{k1 \cdot k2} \bmod p$, which is allocated to the root of tree K_w.

In the following, an example of a key agreement for five subscribers A, B, C, D and E is described with reference to Fig. 3:

In order to establish a common key, subscribers A, B, C, D and E proceed as follows:

- Subscribers A and B carry out a DH process with randomly selected numbers a and b. They obtain the common key $k1=g^{ab} \bmod p$.

- Subscribers C and D carry out a DH process with randomly selected numbers c and d. They obtain the common key $k2=g^{cd} \bmod p$.

- Subscribers A and B on the one side, and subscribers C and D on the other side jointly carry out a second DH process in which subscribers A and B include the common key k1 and subscribers C and D include the common key K2. The result is a common key $k3 = g^{k1 \cdot k2} \bmod p$ for subscribers A, B, C and D.

- Subscribers A, B, C and D on the one side, and subscriber E on the other side carry out a third DH process in which common key k3 of subscribers A, B, C and D and a random number e generated for subscriber E are included. The result is common key $k_w = g^{k3 \cdot e} \bmod p$, which is allocated to the root of the tree K_w.

Owing to the structure of the process according to the

invention, it is possible to include new subscribers or to exclude individual subscribers without having to carry out the entire process again for each subscriber.

The addition of a new subscriber is explained in greater detail with reference to a tree structure having four subscribers according to Fig. 4. The starting situation is a tree structure according to Fig. 2, to which a new subscriber is to be added at leaf B.

When a new subscriber is added to an already existing tree structure which possesses a common secret, in order to establish a new common key for n+1 subscribers, two new leaves B1 and B2 are added at a suitable location of the binary tree (leaf B given). The new tree then has n+1 leaves and is of depth $\lceil \log_2(n+1) \rceil$. The subscriber previously assigned to leaf B is assigned to one of the new leaves B1. The new subscriber is assigned to the other leaf B2 still free. The previous leaf B becomes a node K1 for leaves B1 and B2. Starting from new leaves B1 and B2, new secrets are established as far as the root of the tree only in those nodes K which lie within the framework of the tree structure on the path from new leaves B1 and B2 to the root of the tree K_w. In this specific case, they are nodes K1, K2 and K_w.

If the number of subscribers is a power of two, the depth of the tree is increased through this operation by 1 (see previous example). If the number of subscribers is not a power of two, then, through skillful selection of the leaf to be divided, it is possible to avoid an increase of the depth, as shown by the following example:

In order, for example, to add a fourth subscriber to three subscribers, one proceeds as follows (starting from the situation according to Fig. 1):

- Subscriber C carries out a DH process with newly added subscriber D using randomly generated numbers c` and d (c` should differ from the previously selected c, but this need not be the case). The result is $k2` = g^{c`d} \bmod p$.

- Subscriber A and subscriber B on the one side, and subscribers C and D on the other side carry out a DH process using the values k1 and k2`. The result is $k = g^{k1 \cdot k2`} \bmod p$.

With such a configuration, subscribers A and B need not carry out a new key exchange. Generally, it is only necessary to newly agree upon the secrets which lie in the associated tree on the path from the leaf of the new subscriber to root K_w.

The exclusion or deletion of a subscriber is explained in greater detail with reference to a tree structure having four subscribers according to Fig. 5. The starting situation is a tree structure according to Fig. 2, from which subscriber B is to be removed.

When a subscriber B is excluded or deleted from an already existing tree structure which has a common secret, then, as indicated in Fig. 5, both the leaf of subscriber B who is to be removed and the leaf of subscriber A, assigned to the same common node K1, are removed. Common node K1 becomes new leaf A' of subscriber A remaining in the tree structure. Starting from the leaves of the tree and going as far as root K_w, new secrets are established only in those nodes K which are directly affected by new leaf A' within the framework of the tree structure in the direction of root K_w. In this specific case, this is only root node K_w. Given such a configuration, subscribers C and D need not carry out a

new key exchange. Generally, in this case it is also only necessary to newly agree upon those secrets which lie in the associated tree on the path from the leaf of the partner of the removed subscriber to the root.

The process can be advantageously further developed in many ways: For example, it is possible to use other groups for forming the discrete exponential function $x \rightarrow g^x$.

When a subscriber is added or removed, it is possible, for example, to agree not to use the old secrets, but rather the result of a (possibly randomized) one-way function for the required new implementations of the DH process.

Patent Claims

1. A process for establishing a common cryptographic key for n subscribers using the DH process,
characterized in that
- each of the n subscribers (I) is assigned one leaf of a binary-structured tree which has precisely n leaves and is of depth $\lceil \log_2 n \rceil$;
- for each subscriber (I), a secret (i) is generated and assigned to that leaf of the tree to which the respective subscriber (I) is also assigned;
- secrets are established consecutively in the direction of the tree root for all nodes (K) of the tree, where, starting from the leaves according to the defined tree structure across the entire hierarchy of the tree structure, two already known secrets are always combined via the DH process to form a new common secret and are allocated to a common node (K), so that the last node K_w and therefore the tree root contains the common key of all n subscribers as the secret.

2. The process as recited in Claim 1,
characterized in that
- when a new subscriber is added to an existing tree structure which already has a common secret, in order to establish a common key for n+1 subscribers, two new leaves (B1 and B2) are added as successors to a leaf (B) at a suitable location of the binary tree, so that the new tree has precisely n+1 leaves and is of depth $\lceil \log_2 (n+1) \rceil$;
- the subscriber assigned to the previous leaf (B) and the new subscriber are each assigned to one of the new leaves (B1;B2), the previous leaf B becoming a common node for the new leaves (B1;B2);
- starting from the new leaves (B1;B2) and going as far as the root of the tree, new secrets are established only in those nodes which lie within the framework of the tree

structure on the path from leaves B1 and B2 to the tree root.

3. The process as recited in Claim 1,
characterized in that
- when a subscriber (B) is excluded from an already existing tree structure which already has a secret, both the leaf of the subscriber (B) to be removed as well as the leaf of the subscriber (A) assigned to the same common node are removed;
- the common node becomes the leaf of the subscriber A who is not to be removed, and starting from the leaves of the tree and going as far as the root, new secrets are established only in those nodes which lie within the framework of the tree structure on the path from the new leaf (A) to the tree root.

Abstract

The process is to be such that, even after the group key has been established, subscribers can be removed from or added to the key directory without great effort.

According to the present invention, each of the n subscribers (I) is assigned to one leaf of a binary-structured tree which has precisely n leaves and is of depth $\lceil \log_2 n \rceil$. For each subscriber (I), a secret (i) is generated and is assigned to that leaf of the tree to which the respective subscriber (I) is also assigned. Secrets are established consecutively in the direction of the tree root for all nodes (K) of the tree, two already known secrets always being combined via the DH process to form a new common secret. The last node K_w contains the common key of all n subscribers.

The process of the present invention can be advantageously used to generate a cryptographic key for a group of subscribers whose number is subject to change.

Fig. 1

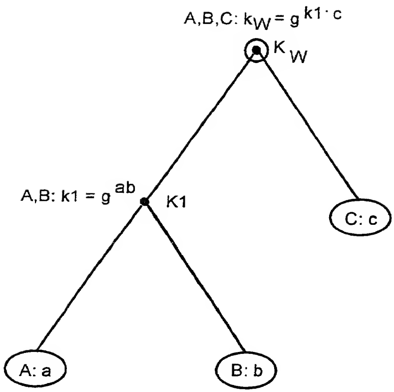


Fig. 1

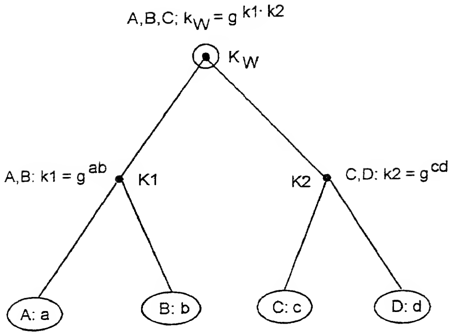


Fig. 2

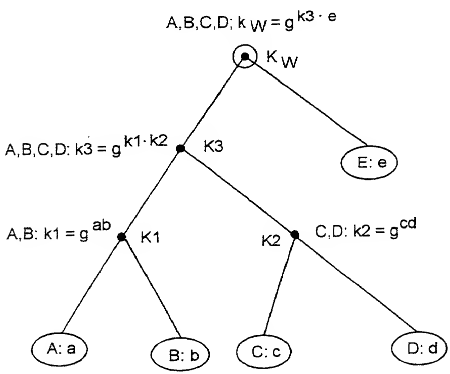


Fig. 3

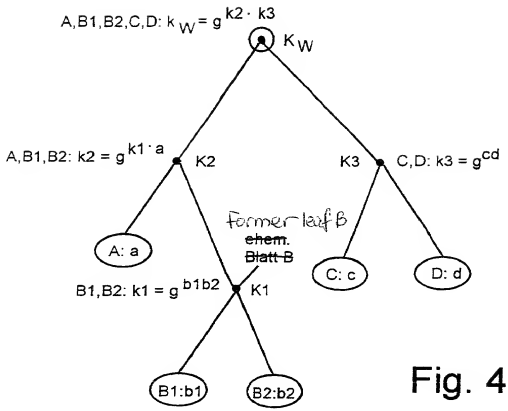

A,B1,B2,C,D: $k_W = g^{k2 \cdot k3}$
K_W
A,B1,B2: $k2 = g^{k1 \cdot a}$
K2
K3
C,D: $k3 = g^{cd}$
Former leaf B
~~chem. Blatt B~~
A: a
C: c
D: d
B1,B2: $k1 = g^{b1b2}$
K1
B1:b1
B2:b2

Fig. 4

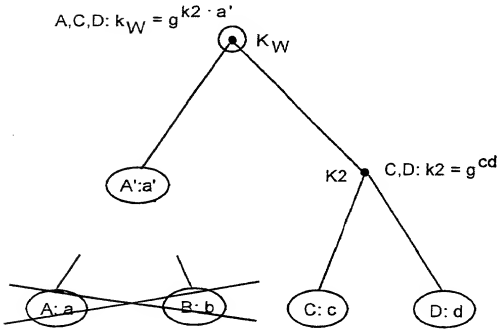

A,C,D: $k_W = g^{k2 \cdot a'}$
K_W
A':a'
K2
C,D: $k2 = g^{cd}$
A: a
B: b
C: c
D: d

Fig. 5

[2345/152]

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **PROCESS FOR ESTABLISHING A COMMON CRYPTOGRAPHIC KEY FOR N SUBSCRIBERS**, the specification of which was filed as International Application No. PCT/EP99/07051 on September 22, 1999 and as U.S. Application Serial No. 09/807181 on April 9, 2001.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
198 47 941.7	Fed. Rep. of Germany	09 October 1998	Yes

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004
CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Joerg SCHWENK**

Inventor's Signature: Joerg Schwenk

Date: 5. June 2001

Residence: Suedwestring 27
64807 Dieburg DEX
Federal Republic of Germany

Citizenship: German

Post Office Address: Same as above.